Проактивное обнаружение
схем мошенничества

Kaspersky Fraud Prevention

kaspersky активируй будущее

Кибермошенничество — один из популярных видов киберпреступлений. Его основная цель — причинение материального или другого ущерба путем хищения с помощью цифровых технологий личной информации пользователей.

Баланс между защитой от кибермошенничества и удобством пользователей

Ландшафт киберугроз для бизнеса постоянно меняется — появляются всё новые векторы атак, мошенники используют схемы обмана, о которых еще недавно никто не знал. Для компаний, оказывающих цифровые услуги, одна из самых сложных задач заключается в том, чтобы обеспечить удобство работы клиентов, одновременно защитив их данные и средства, в том числе от неосторожности самих пользователей.

В век цифровой трансформации компании переносят в онлайн всё больше услуг и стараются сделать взаимодействие пользователей с сервисами максимально быстрым и удобным. Однако масштабные процессы цифровизации ставят под угрозу данные пользователей из-за их доступности, что привлекает мошенников. Часто они совершают атаки, пользуясь доверием клиентов к компании.

Угрозы для бизнеса

Цифровые технологии и онлайн-каналы стали не только неотъемлемой частью развития бизнеса и клиентского сервиса, но и создали новые векторы киберугроз для организаций. Наличие мошеннической активности на веб-сайтах и в мобильных приложениях ведет к дополнительным затратам и рискам.

Прямые финансовые потери

- Возмещение украденных средств пользователям
- Возмещение chargeback партнерам (мерчантам)
- Санкции за несоблюдение требований регуляторов (ПОД / ФТ, СБП)
- Затраты на второй фактор аутентификации для добросовестных пользователей

Косвенные издержки

- Затраты на претензионную работу, колл-центр и расследования
- Расходы на маркетинговые акции, которыми злоупотребляют специально созданные аккаунты
- Упущенная прибыль из-за нецелевого использования программ лояльности
- Непрогнозируемые нагрузки из-за бот-активности
- Репутационные и юридические риски

Несоответствие ожиданиям клиентов

- Дополнительные шаги проверки для пользователей
- Негативный опыт при взломе учетной записи и данных внутри личного кабинета
- Использование мошенниками накопленных бонусов в программах лояльности

О решении

Kaspersky Fraud Prevention — решение для проактивного обнаружения даже самых сложных схем мошенничества в режиме реального времени в цифровых каналах — на веб-сайтах и в мобильных приложениях.

Продукт состоит из двух самостоятельных модулей — Advanced Authentication и Automated Fraud Analytics, комбинация которых делает решение максимально эффективным.

Kaspersky Fraud Prevention

Advanced Authentication

Automated Fraud Analytics

Advanced Authentication

Оценка риска сессии пользователя (Risk-Based Authentication, RBA) с помощью технологии непрерывной аутентификации для быстрого принятия решений на критичных этапах, таких как вход, регистрация, смена пароля, изменение данных. Формирует ответ по API в виде светофора (зеленый, серый и красный) для каждого пользователя.

Ключевые возможности

Защита учетной записи от кражи и мошеннических действий

Сокращение затрат на второй фактор аутентификации для добросовестных пользователей

Быстрое формирование RBA-вердикта — до 1 секунды

Удобный конструктор настройки правил

Защита от вмешательства в работу решения на стороне Frontend

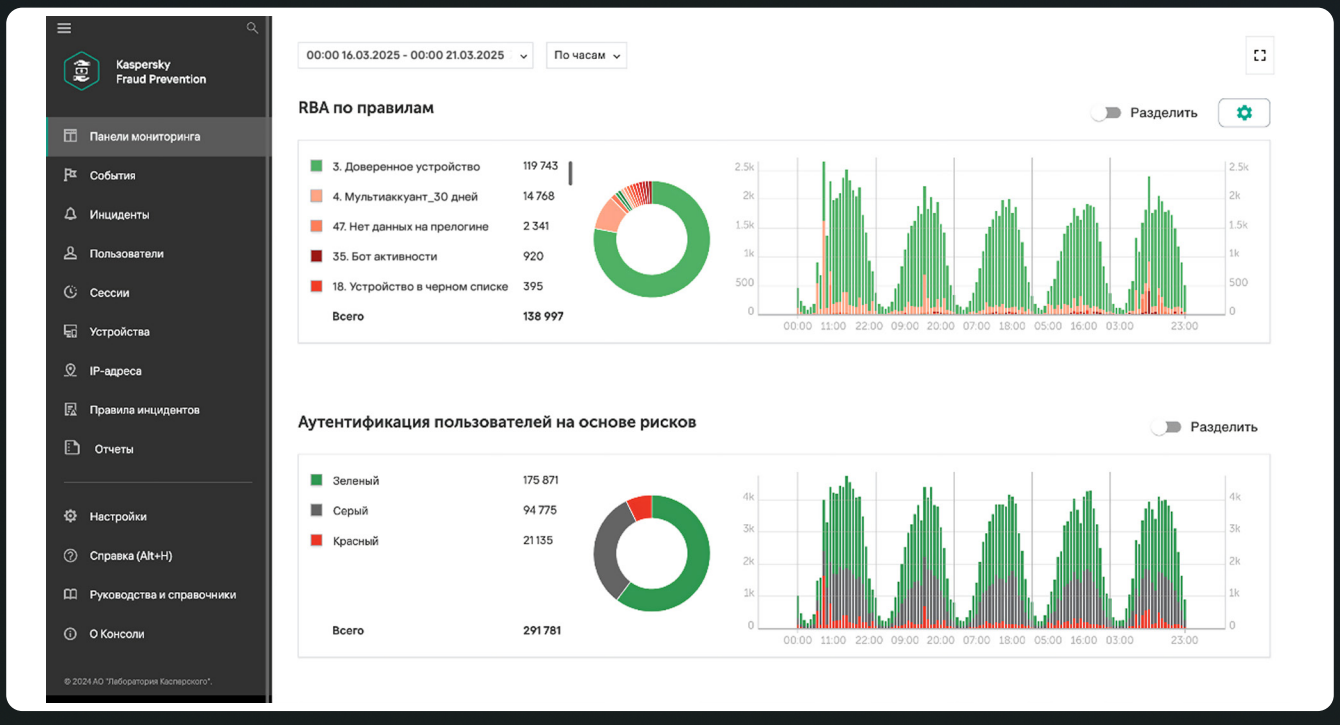
Улучшение клиентского пути для доверенных пользователей

Возможность использования дополнительных данных от заказчика для построения более сложных правил

Обогащение техническими данными собственных аналитических систем

Расширение спектра обнаружения угроз при использовании модуля Automated Fraud Analytics

Удобный и понятный интерфейс



Automated Fraud Analytics

Непрерывный анализ действий пользователя на вашем онлайн-сервисе в режиме реального времени для обнаружения подозрительных активностей, а также создание инцидентов.

Ключевые возможности

Обнаружение аномалий и отправка инцидентов в режиме реального времени

Идентификация компрометации аккаунта, мошеннических аккаунтов и отмывания денежных средств

Подробная аналитика по инцидентам и связям для расследования

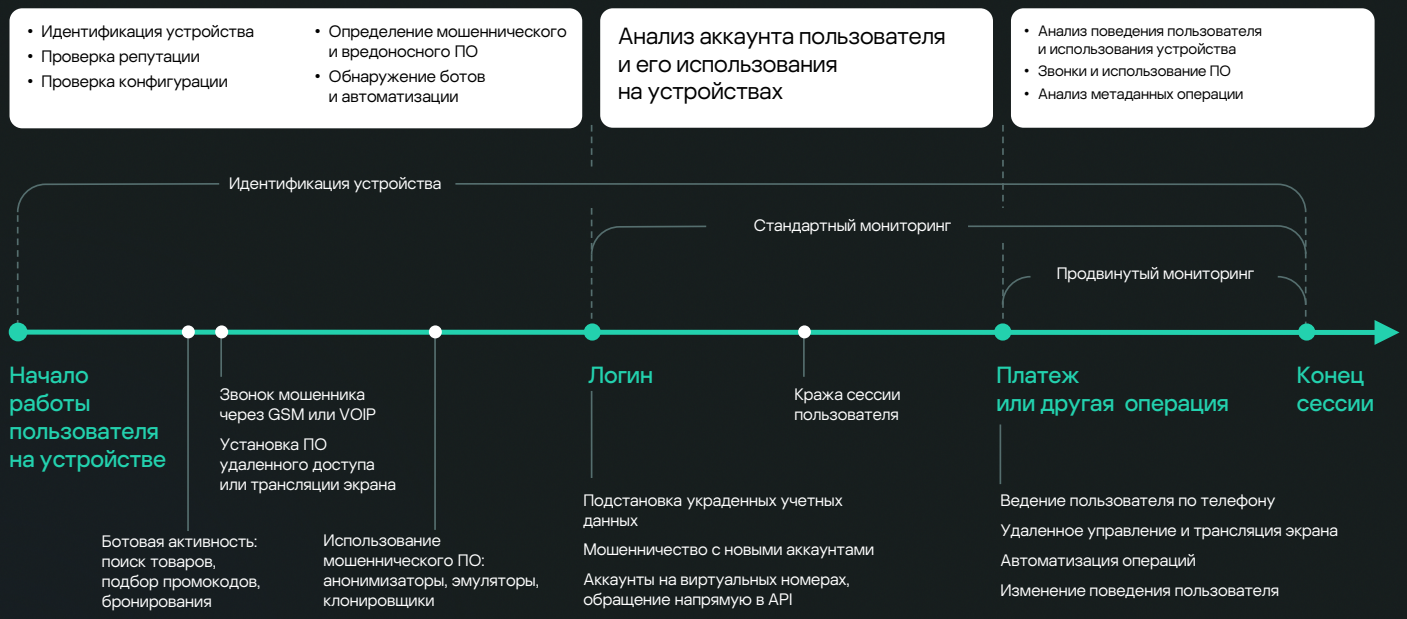
Обогащение данными собственных аналитических систем

Гибкий движок правил для выявления даже самых сложных схем

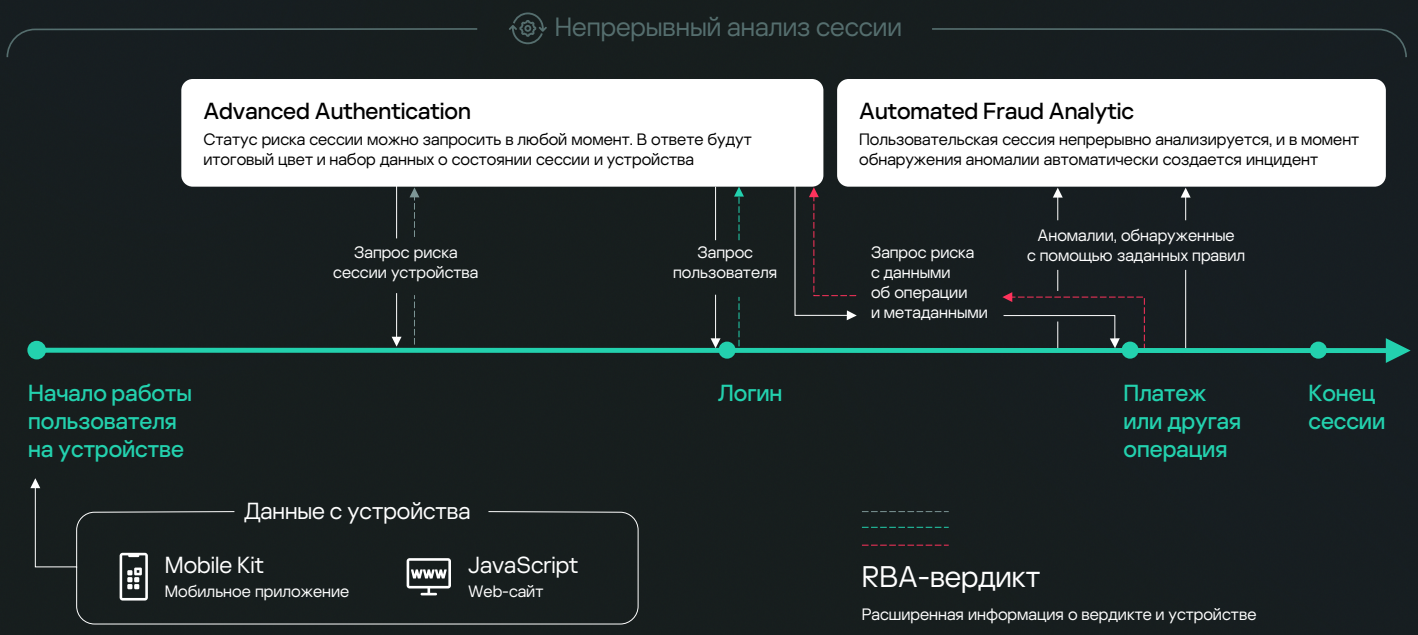
Удобный и понятный интерфейс

Непрерывный анализ сессии

Поддерживаем короткие и длинные сессии



Взаимодействие с Kaspersky Fraud Prevention



Сценарии использования Kaspersky Fraud Prevention

Kaspersky Fraud Prevention позволяет добиться оптимального баланса между уровнем безопасности и удобством для клиентов благодаря комбинации современных технологий, многолетней антифрод-экспертизы и встроенного машинного обучения.

Обнаруживает кражу учетных записей пользователей, несанкционированный доступ и мошеннические аккаунты

Выявляет телефонное мошенничество с использованием социальной инженерии, в том числе из мессенджеров

Позволяет обнаруживать схемы отмывания денежных средств и мошеннические кластеры

Обнаруживает злоупотребление маркетинговыми акциями и программами лояльности

Позволяет улучшить клиентский опыт и повышает доверие к компании

Повышает эффективность фрод-мониторинга при помощи обогащения дополнительными данными

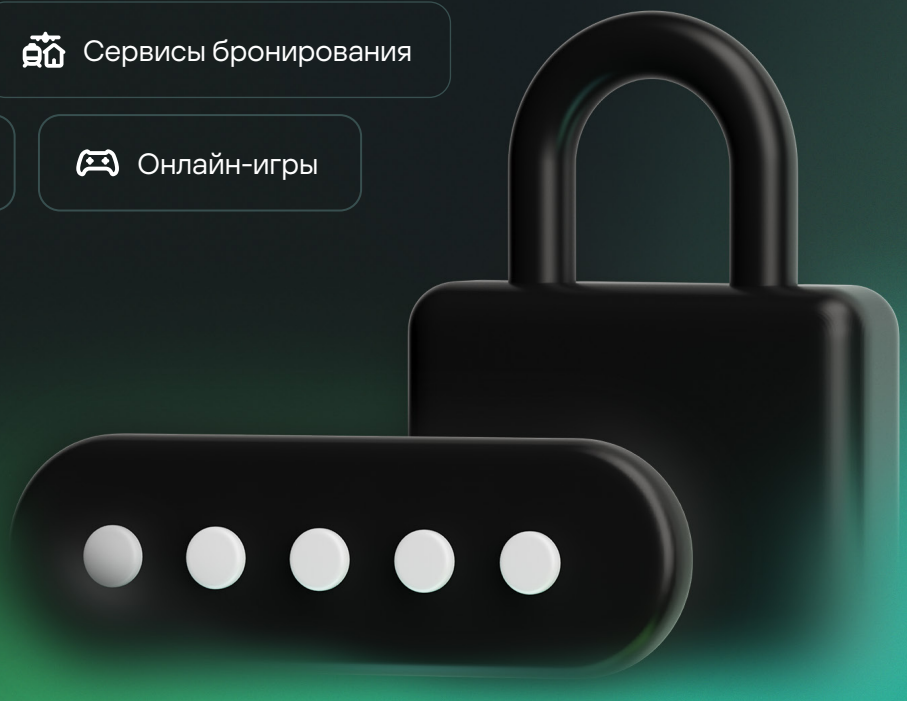
Позволяет соответствовать требованиям регуляторов

Снижает затраты на претензионную работу и расходы на второй фактор аутентификации (СМС, пуш-уведомления и пр.)

Сферы применения

Для любых компаний, предоставляющих онлайн-сервис пользователям.

- Финансовые организации
- Торговля
- Программы лояльности
- Государственные сервисы
- Сервисы бронирования
- Медицина
- Телеком
- Онлайн-игры



Преимущества Kaspersky Fraud Prevention

> 10 лет

в обнаружении мошенничества и разработке антифрод-технологий

> 290

параметров обнаружения в конструкторе правил — для выявления сложных и постоянно меняющихся схем мошенничества

Мониторинг

Непрерывный анализ устройства и окружения, поведения пользователя и его взаимодействия с устройством

Защита

Надежная схема интеграции, затрудняющая обход антифрод-системы

Технологии

Продукт разработан «Лабораторией Касперского» без использования сторонних решений и входит в реестр отечественного ПО

Адаптивность

Прозрачность и гибкость настройки правил для генерации инцидентов и отправки вердиктов в системы заказчика

Полная поддержка клиентов

От этапа интеграции и персональных настроек для каждого клиента до проведения расследования мошенничества по запросу

Нативная интеграция с продуктами «Лаборатории Касперского»:

Лицензирование, модель поставок и техническая поддержка

Варианты размещения

Облако
Базовый сценарий

Частное облако / Мощности заказчика
Индивидуальные условия по запросу

Техническая поддержка

- Стандартная
- Расширенная

Лицензирование

Осуществляется по модулям на 1, 2 и 3 года. При увеличении пользователей сайта и / или мобильного приложения цена становится выгоднее.

Этапы внедрения Kaspersky Fraud Prevention

1. Подготовка и предоставление сенсоров для веб- и мобильного каналов
   - Лаборатория Касперского
2. Интеграция сенсоров в онлайн-каналы
   - Заказчик
3. Настройка базовых правил
   - Лаборатория Касперского
4. Сбор данных (обычно занимает 2-3 недели)
   - Лаборатория Касперского
5. Донастройка и анализ качественных результатов

Технологическое лидерство и экспертиза мирового уровня

Kaspersky Fraud Prevention опирается на знания, технологии и профессионализм **четырех из пяти Центров экспертизы компании.**

Мы анализируем кибермошенничество по всему миру, исследуем новые мошеннические схемы и угрозы

Применяем алгоритмы машинного обучения в продукте, предоставляем услуги по расследованию инцидентов и даем рекомендации по реагированию и минимизации последствий

Kaspersky Fraud Prevention

Подробнее

kfp@kaspersky.com
www.kaspersky.ru

#kaspersky
#активируйбудущее